UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,699	03/27/2001	Doug L. Rollins	MTIPAT.187A	9926

20995 7590 08/12/2008

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

NOTIFICATION DATE	DELIVERY MODE
08/12/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com
eOAPilot@kmob.com

Office Action Summary	Application No.	Applicant(s)	
	09/818,699	ROLLINS, DOUG L.	
	Examiner	Art Unit	
	MINH DIEU NGUYEN	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,7,8,12-14,17 and 20-24* is/are pending in the application.

4a) Of the above claim(s) *2-4,6,9-11,15,16,18 and 19* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,7,8,12-14,17 and 20-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/12/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/12/08 has been entered.

2. Claims 1, 5, 7-8, 12-14, 17 and 20-24 are pending.

Information Disclosure Statement

3. The information disclosure statement filed 6/12/2008 has been placed in the application file and the information referred to therein has been considered as to the merits.

Response to Arguments

4. Applicant's arguments filed 6/12/08 have been fully considered but they are not persuasive. The Applicant argues that Hanna teaches away from the claims invention by providing a system where multiple authorized users can have access to the same encrypted data by including decryption key information with the encrypted data to which they have access. The Examiner respectfully disagrees, Hanna discloses several embodiments where a client issues a request to the file server to access data (Hanna:

col. 5, lines 15-16) as well as group of clients may obtain access to the encrypted data (Hanna: col. 6, lines 47-48). In particular, Hanna discloses after encrypting data F, the client Ca encrypts the first decryption key K1d with a second decryption key K2d **known to the client Ca.** The second encryption key K2e comprises the public key of a public key pair **owned by the client Ca**. Thus, the encrypted first decryption key **can only be decrypted by the client which owns or has access to the private key of the public key pair, which typically would be only client Ca** (Hanna: col. 4, lines 59-67, col. 5, lines 15-32). In this manner, Hanna indeed discloses the data is encrypted differently via the first client computer than by other client computers and only the first client computer who has access to the private key is able to decrypt the encrypted data.

On the same argument, the Applicant submits Pond discloses much of the data necessary to decrypt an encrypted file is attached permanently to the file. On the same line of response, the Examiner disagrees, even when at least one of the key stream flags of the key mix must be set, the key mix itself is not enough to decrypt the information because the key mix is utilized to designate which keys, in addition to the Mandatory Key, are to be used for encryption and decryption of the protected file (Pond: col. 3, lines 45-48), further the key mix is encrypted using the mandatory key (as submitted by the applicant, Pond: col. 4, lines 17-19) (i.e. encrypted information only yields gibberish, unintelligible data to unauthorized parties, as such it is without data indicative of an associated decryption key).

In response to applicant's arguments against the references individually (i.e. Fan (6,310,692) and Simmons et al. (2001/0039659)), one cannot show nonobviousness by

attacking references individually where the rejections are based on combinations of references. Fan is relied on for the teaching of generating and transmitting a notification message, Fan is not relied on to describe encryption or decryption protocols as submitted by the Applicant. See In re Keller, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); In re Merck & Co., 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The Applicant argues that Eldridge fails to disclose other limitations of the base claims. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Objections

5. Claims 1, 8 and 22 are objected to because of the following informalities:

a) As to claim 1, "wherein the client computer system uniquely retains a private key uniquely associated with the client computer system.." should be -- wherein the **first** client computer system uniquely retains a private key uniquely associated with the **first** client computer system..--.

b) As to claim 8, “wherein the client computer system retains a private decryption key that is unique to the client computer system” should be -- wherein the **first** client computer system retains a private decryption key that is unique to the **first** client computer system--.

c) As to claim 22, "the first client computer system is uniquely associated with the client computer system" should be --the first client computer system is uniquely associated with the **first** client computer system--

Appropriate correction is required.

Specification

6. The amendment filed 11/7/2007 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: "the client computer system uniquely retains a private key" and "wherein both the encryption key and the private key are needed for decryption of encrypted data".

Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

8. Claims 1 and 5 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed,

had possession of the claimed invention. There is no support for the amended limitation “the client computer system uniquely retains a private key” and "wherein both the encryption key and the private key are needed for decryption of encrypted data” in claim 1 and “wherein both the public and the private encryption keys are needed to decrypt encrypted data” in claim 5. At best, paragraph 0046 indicates that other users will not have access to the private key of the user that originally encrypted and stored the file, there is no indication on the computer system uniquely retains a private key and paragraph 0019 discloses a pair of keys, where one is used for encryption, and the other for decryption. There is no mention on both encryption (public) key and private key are needed to decrypt encrypted data”.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 5, 8, 12-13, 17, 20-22 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna et al. (7,178,021) in view of Pond et al. (4,864,616) in view of Simmons et al. (2001/0039659) and further in view of Fan et al. (6,310,692).

a) As to claims 1 and 8, Hanna discloses a method of transferring data over a computer network from a network server to a client computer system (Hanna: col. 1, lines 17-20), the method comprising: receiving a request by a requestor using a first

client computer system (Hanna; col. 5, lines 15-16) for data from at least one network server storing data, at least some of the data stored by the network server being encrypted (Hanna: col. 4, lines 16-21); if the requested data is encrypted with the encryption key, sending the encrypted data to the first client computer system (i.e. the encrypted first decryption key along with the encrypted data are sent to the client, where the first decryption key is encrypted with the public key of client (Hanna: col. 5, lines 21-24), the decryption key is not sent in the clear, the transmitted encrypted decryption key is gibberish, unintelligible data to unauthorized parties) wherein the first client computer system uniquely retains a private key uniquely associated with the first client computer system such that other client systems do not have access to the private key and wherein both the encryption key and the private key are needed for decryption of encrypted data (i.e. after encrypting data F, the client Ca encrypts the first decryption key K1d with a second decryption key K2d known to the client Ca. The second encryption key K2e comprises the public key of a public key pair owned by the client Ca. Thus, the encrypted first decryption key can only be decrypted by the client who owns or has access to the private key of the public key pair, which typically would be only client Ca, Hanna: col. 4, lines 59-67; col. 5, lines 15-32), the first and second encryption key and the first and second decryption key comprise public and private keys where the requesting client decrypts the encrypted first decryption key with the private key of its public key pair and utilizes the decrypted first decryption key to decrypt the encrypted data F, Hanna: col. 4, lines 54-67; col. 6, lines 2-6).

Hanna is silent on the capability of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key.

Pond is relied on for the teaching of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key (i.e. the system checks to see if a banner is present, wherein a banner indicates if the file is protected, Pond: col. 3, lines 43-44; col. 8, lines 26-27).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of checking an attribute of the requested data to determine whether the requested data is encrypted with an encryption key in the system of Hanna, as Pond teaches, so as to protect sensitive data files with proper labels (Pond: col. 1, lines 6-10).

The combination of Hanna and Pond is silent on the capability of if the requested data is unencrypted (see Pond), automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data.

Simmons is relied on for the teaching of automatically retrieving the encryption key associated with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data (Simmons: 0016, 0041, 0046).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of automatically retrieving the encryption key associated

with the requestor from the client computer system; encrypting the requested data with the encryption key associated with the requestor automatically and without user intervention to create encrypted data in the system of Hanna and Pond, as Simmons teaches, so as to securely protect transmitted data over a network.

The combination of Hanna, Pond and Simmons is silent on the capability of sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor.

Fan is relied on for the teaching sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor (i.e. notification is generated and transmitted, Fan: col. 5, lines 45-49. It is obvious that what is in the notification is purely the design choice).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending a message to the requestor indicating that the requested data is not encrypted with their key when the encryption key used to encrypt the requested data is not associated with the requestor in the system of Hanna, Pond and Simmons, as Fan teaches, so as to dynamically managing resources (Fan: col. 1, lines 8-12).

b) As to claim 5, the majority of this claim is in claim 1 with the addition of the following limitation: automatically generating independently of information from a network server a public encryption key and a corresponding private encryption key in a

client computer system; storing the public encryption key and the corresponding private encryption key in the client computer system (Simmons: 0041). Pond discloses associating an attribute with a data file, the attribute indicating whether the data file is encrypted (Pond: col. 3, lines 43-44; col. 8, lines 26-27), and the attribute indicating an owner of the public encryption key (Hanna: col. 5, lines 4-6). Hanna discloses public and private encryption key where the data file is encrypted with public key (Hanna: col. 4, lines 53-57).

c) As to claims 12, 17 and 20, the combination of Hanna, Pond, Simmons and Fan discloses the method of claim 1, further comprising sending the requested data to the client computer system only if the requested data is encrypted and if the requestor is the owner of the encryption key (Hanna: col. 5, lines 19-25).

d) As to claims 13, 21-22 and 24, the combination of Hanna, Pond, Simmons and Fan discloses the method of claim 1, wherein the encryption key is derived at least in part from an identification code, identification code is uniquely associated with the first client computer system, Pond: col. 5, lines 20-40).

11. Claims 7, 14 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanna et al. (7,178,021) in view of Pond et al. (4,864,616) in view of Simmons et al. (2001/0039659) in view of Fan et al. (6,310,692) and further in view of Eldridge et al. (6,094,721).

The combination of Hanna, Pond, Simmons and Fan does not explicitly disclose the public and private keys are based on a password.

Eldridge discloses a method and apparatus for updating the password status of one of more servers in a client/server environment comprising public and corresponding private key derived from password (Eldridge: col. 5, lines 33-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of generating public and private key from a password as Elridge teaches in the system of Hanna, Pond, Simmons and Fan so as to secure password authentication to access (Elridge: col. 1, lines 15-17).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2137